

A new deep steganographic technique for hiding several secret images in one cover

Mohamed Htiti¹, Aziza El Ouazizi², Ismail Akharraz³, Abdelaziz Ahaitouf¹

¹Laboratory of Engineering Sciences (LSI), Faculty of Taza Polydiscipline, University of Sidi Mohamed Ben Abdellah, Fez, Morocco

²Laboratory of Artificial Intelligence, Data Sciences and Emergent Systems (LIASSE), National School of Engineers (ENSA), University of Sidi Mohamed Ben Abdellah, Fez, Morocco

³Laboratory of Mathematical and Informatics Engineering, University of Ibnou Zohr, Agadir, Morocco

Article Info

Article history:

Received Sep 16, 2024

Revised Jan 5, 2025

Accepted Jan 27, 2025

Keywords:

Convolutional neural network

Deep learning

Deep steganography

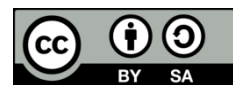
Digital data security

Image steganography

ABSTRACT

Deep learning has been integrated with image steganography to enhance steganographic security by automatically acquiring the ability to hide information. The issue with current models is that if the cover image is accessible, it is possible to expose the hidden information by simply calculating the differences between the cover image and the steganographic image. This paper introduces a novel image steganography model that utilizes convolutional neural network (CNN) to enhance the dissimulation and extraction capabilities. Specifically, we propose a model that hides two images in a single cover image. Before being hidden within the cover image, a random pixel image is generated and combined with the real secret image. Experimental results show that our proposed method is more effective and relevant.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Mohamed Htiti

Laboratory of Engineering Sciences (LSI), Faculty of Taza Polydiscipline

University of Sidi Mohamed Ben Abdellah

Fez, Morocco

Email: mohamed.htiti1@usmba.ac.ma

1. INTRODUCTION

Information security relies on three fundamental categories: watermarking, cryptography, and steganography. Watermarking is mainly used to protect copyright and create electronic signatures [1] while cryptography is essential for maintaining the confidentiality, integrity, and authentication of data in public communications, offering strong protection [2]. Steganography involves hiding information within other content to transmit data without drawing attention to the concealed message [3]. Images are commonly used in steganography due to their high capacity to contain data, their popularity, and the possibility of hiding information invisibly from the human eye. Every digital image, especially high-resolution ones, contains numerous pixels and color components, enabling bits to be modified without visibly altering the image. In addition, there is a high degree of correlation between adjacent pixels in an image, enabling data to be hidden imperceptibly by slightly altering the values of individual pixels. Images also offer data redundancy and are highly resistant to certain compressions, as in lossless formats such as PNG, enabling hidden data to be recovered even after manipulation. Their omnipresence in digital communications and their easy transmission make them an ideal medium for discreetly hiding information. In the context of images, steganography involves embedding secret information in a cover image. An image steganography algorithm consists of two parts. The first part is used to hide a confidential message inside the cover image. The second

part is an extraction algorithm designed to recover of the secret message from the stego image (the cover image containing the secret) [4].

Currently, there are two categories of steganographic algorithms, namely classical techniques and machine learning techniques. In the first categories, we find domain spatial techniques where the secret information bits are embedded directly in the pixels of the cover image. Several research projects have been carried out to improve the techniques of this approach, including the least significant bit (LSB) technique [5]–[10], where the secret bits are generally hidden in the LSB of the cover pixels. Another technique called pixel value differencing (PVD) involves discreetly altering the pixel values of an image to encode the hidden information. This is achieved by making small modifications to the disparity values of adjacent pixels to encode the desired data bits [11]–[14]. Another important type of classical technique is the transform domain. The initial step is to transform the cover image into the frequency domain, and the secret information is then hidden in the wavelet. Several research projects have been carried out to improve the performance of this approach. The discrete cosine transform (DCT) technique has undergone several improvements and implementations in this work, [15]–[18]. Similarly, the discrete wavelet transform (DWT) technique has also been explored [19]. In the second category, which utilizes artificial intelligence, existing research shows promise for information security because it preserves the visual and statistical properties of cover images with effective hiding of secret information. Indeed, unlike traditional steganography, which often focuses on modifying the characteristics or pixels of the cover image to incorporate secret data, deep steganography uses neural networks to generate images containing hidden information. This offers potentially more robust and sophisticated concealment capabilities, as neural networks can learn complex patterns and representations. Deep steganography takes advantage of the strengths of machine learning, enabling the process of hiding and extracting confidential data to be learned automatically.

Several artificial intelligence tools have been employed by researchers in the field of deep steganography, such as genetic algorithms [20], generative adversarial networks [21], and convolutional neural network (CNN) autoencoder; Baluja [22] who use deep neural networks to hide a color image inside another image of the same size, demonstrating the ability of the deep learning method in image hiding. Baluja's problem is that it is possible for an attacker to obtain the original cover image (C) without the embedded secret image. In this case, it becomes possible to partially reveal the secret image by comparing the original cover image (C) with the sent image (C') by plotting their difference $|C-C'|$. Baluja [23], while suggesting concealing multiple images within a single image, initially trained his model to embed one image in one cover. The model identifies the optimal locations for embedding the hidden information and decides how to compress and represent it. Subsequently, the author proposed utilizing the resulting model to compress and conceal two images within one cover.

In this paper, we propose a new architecture that hides two secret images rather than just one in the cover image. After training our model, it should be able to hide two secret images within a single cover image. Before implementing this, we suggest a technique to enhance the solution's performance by randomly generating a fake secret image and embedding it alongside the real secret in the cover image. The rest of the paper is structured as follows: section 2 describes the problematic aspects related to the topic and highlights our specific contributions. Results and discussions are presented in section 3. Finally, in section 4, we give the conclusion and perspectives of our study.

2. PROPOSED METHOD

Baluja [23] has succeeded in hiding an original color image (S) inside another cover image (C), the result being the stegano image (C'). However, it is possible for an attacker to obtain the original cover image (C) without the embedded secret image. In this case, it becomes possible to partially reveal the secret image by comparing the original cover photo (C) with the sent photo (C') by calculating their difference. An example of Baluja's model is shown in Figure 1, which illustrates how the difference between (C) and (C') can reveal the secret. Column 3 represents the Stegano image, which is simply the secret image displayed in column 2 and embedded in the cover image in column 1. The extracted secret is shown in column 4. By comparing the cover image (C) and the stegano image (C') in column 5, we can see that the secret hidden in the stego image is visible. When a steganalyst obtains images C and C', he can determine the secret by calculating the difference between them $|C-C'|$.

One solution, suggested by Sharma *et al.* [24], is to integrate a block permutation onto the secret image before incorporating it into the learning process. Figure 2 shows an example of block permutation applied to an image. Since he considered the permutation he performed to be a form of cryptography, he applied cryptographic criteria to his results. In addition, his model is trained on a database of permuted images, which further increases the computational complexity. In other words: i) during the prediction stage: using this model implies using both the permutation and dissimulation algorithms and ii) during the reception

stage: it is necessary to use the extraction algorithm and the permutating canceling algorithm, as shown in Figure 3.

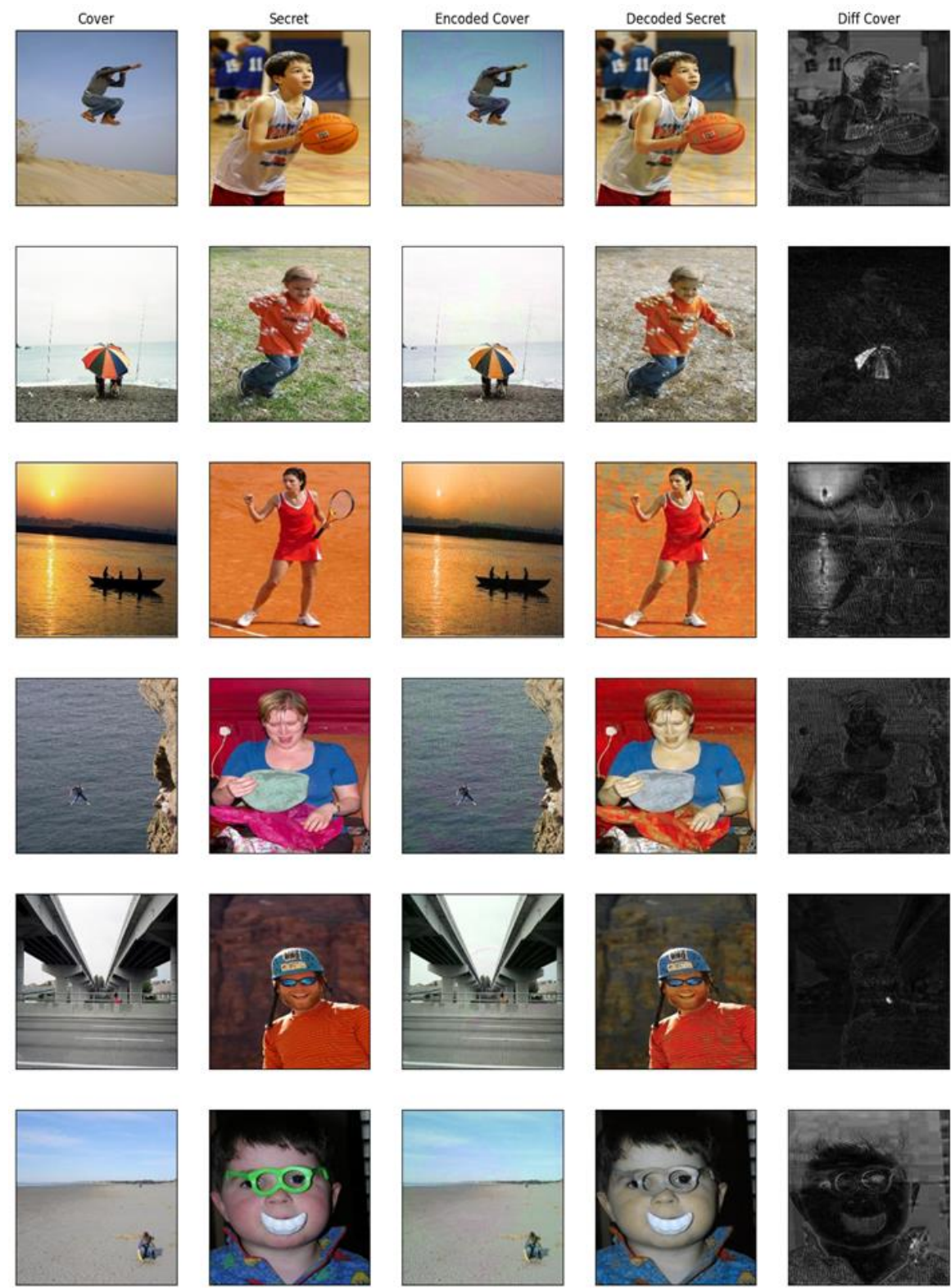


Figure 1. Results using the Baluja's model



Figure 2. Example of Sharma permutation

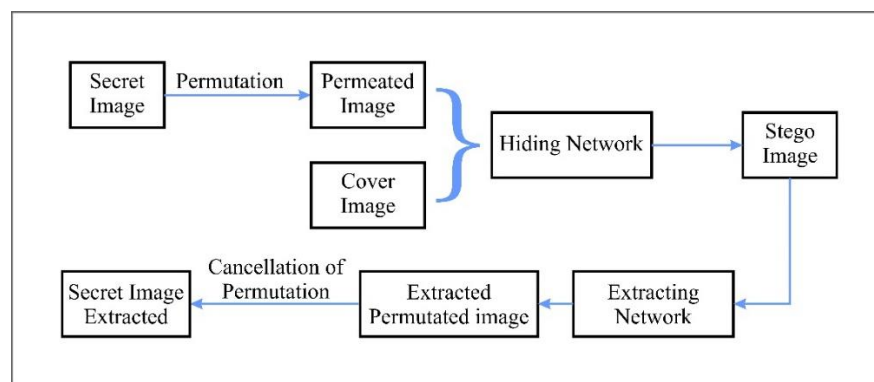


Figure 3. Sharma model

We propose hiding several secret images in a single cover image rather than including a permutation or cryptographic layer that complicates the computation. To enhance dissimulation quality, we propose a novel CNN-based model that trained to hide a randomly generated image and the secret image in one cover image. This approach introduces complexity and masks the secret image features, making it more challenging for attackers to detect or extract.

Figure 4 illustrates the general principle of the proposed architecture. The structure of the network in question resembles that of autoencoders. In general, encoders attempt to make an output that is very close to the input after a number of changes. This process enables them to learn the fundamental characteristics of the input images. However, in our case, instead of just reproducing images, the network has the additional task of hiding two images while simultaneously generating another image (stego image). The preparation layer adds Gaussian noise to (the secret S +random image). This layer prevents the model from storing information in LSB bits. Next, we concatenate the input images with the cover C . The second layer consists of the hiding network, which takes the output of the preparation layer as input to generate the stego image C' .

This network comprises 10 convolution layers, each made up of three parallel sub-layers with 128 filters of sizes (3×3) , (4×4) , and (5×5) respectively. The third layer is the revelation network, which takes the stego image exclusively as input. This network is responsible for removing the cover image to reveal the secret image S' .

The model was trained using Python 3 Google Compute Engine on the Google Colab platform, which provides access to additional resources, including graphics processing unit (GPU) and random access memory (RAM). Google Colab also provides a JupyterLab environment in which model development can take place. This environment also provides access to all the essential libraries for artificial intelligence and machine learning, including Keras, Matplotlib, Numpy, and Scipy.

The Flickr30k database was used to train the model. The images in the dataset were reduced to 256×256 according to our training model because their sizes were irregular throughout the dataset. A total of 1000 covers, 1000 secrets, and 1000 random images were used in the training process.

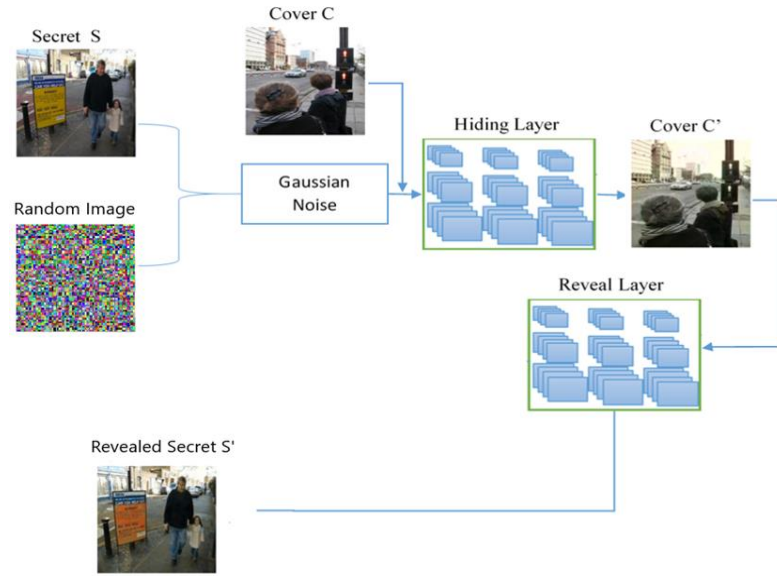


Figure 4. Proposed architecture

3. RESULTS AND DISCUSSION

In most cases, imperceptibility can be determined by comparing the pixel values of the original image with those of the stego image. The result is shown in Figure 5; column 1 shows the cover images, columns 2 and 3 represent the true secrets and random images respectively. Columns 4 and 5 contain the stegano image and the extracted secret image. Column 6 shows the $|C-C'|$ difference. We can see that there is no trace of the secret in the images in the “Diff cover” column. Visually, our model is more successful than Baluja's. Reliable tools are crucial for assessing the quality and imperceptibility of steganographic images. Various indicators are used for this purpose, including peak signal-to-noise ratio (PSNR), universal image quality index (UIQI), blind/referenceless image spatial quality evaluator (BRISQUE) score, and structural similarity index measure (SSIM). Here's a detailed presentation of each of these indicators:

3.1. Peak signal-to-noise ratio

PSNR is an indicator commonly used to assess the level of noise present in the pixels of a steganographic image, in order to measure its imperceptibility. Steganographic images of excellent quality have a PSNR value of 40 dB or more, while those with a value of less than 30 dB are considered to be of inferior quality. PSNR is calculated using logarithmic values of mean square error (MSE) [25] and I_{max}^2 represents the highest pixel value in the image.

$$PSNR = 10 \log_{10} \left(\frac{I_{max}^2}{MSE} \right) \quad (1)$$

3.2. Universal image quality index

This index is used to evaluate the variations present in the steganographic image compared to the original image. This method divides the image comparison into three distinct parts: i) luminance comparison (LC), ii) contrast comparison (CC), and iii) structural comparison (SC). The UIQI index varies between -1 and 1, the best value being 1 [26]:

$$L(X, Y) = \frac{2\mu_X\mu_Y}{\mu_X^2 + \mu_Y^2} \quad (2)$$

$$C(X, Y) = \frac{2\sigma_X\sigma_Y}{\sigma_X^2 + \sigma_Y^2} \quad (3)$$

$$S(X, Y) = \frac{2\sigma_{XY}}{\sigma_X + \sigma_Y} \quad (4)$$

$$UIQI(X, Y) = L(X, Y) * C(X, Y) * S(X, Y) \quad (5)$$

Where X represents the cover image, Y represents the stego image, μX represents the mean value of the X matrix, μY represents the mean value of the Y , σX represents the standard deviation of the X matrix, σY represents the standard deviation of the Y matrix, and σXY represents the covariance between the X and Y matrices.

3.3. Blind/referenceless image spatial quality evaluator score

The BRISQUE score [27] is a statistical measurement of the natural scene, excluding reference images such as PSNR and SSIM. It ranges from 0 to 100, with the best score being the lowest. The score is calculated using the support vector regression (SVR) model and difference mean opinion score (DMOS). It is widely used in image steganography research.

3.4. Structural similarity index

The SSIM is a metric used to evaluate the imperceptibility of steganographic images. Unlike PSNR, which relies on a summation method, SSIM focuses on three key factors: luminance, contrast, and structure, providing a more comprehensive assessment of image quality. In red, green, and blue (RGB) color images, the SSIM can be mathematically defined using (6). The first component, $L(im, im')$, is responsible for comparing the luminance levels between two images, im and im' . This luminance comparison reaches its maximum value of 1 when the luminance of both images is identical. The maximum value of $c(im, im')$ is 1, which occurs when the contrasts of the two images, calculated based on their standard deviations (σ), are equal. The third component, $S(im, im')$, compares the structural similarity between two images im and im' based on their correlation coefficient. The maximum possible value for SSIM is 1, with the overall range of SSIM values falling between 0 and 1. To prevent division by zero, constant values C_1 , C_2 , C_3 are introduced in the formula. It is recommended to use the values $C_1=(0.01 \times 255)^2$, $C_2=(0.03 \times 255)^2$, and $C_3=C_2/2$ as the default value [28].

$$SSIM(im, im') = l(im, im')c(im, im')s(im, im') \quad (6)$$

$$l(im, im') = \frac{2\mu_{im}\mu_{im'} + C_1}{\mu_{im}^2 + \mu_{im'}^2 + C_1} \quad (7)$$

$$c(im, im') = \frac{2\sigma_{im}\sigma_{im'} + C_2}{\sigma_{im}^2 + \sigma_{im'}^2 + C_2} \quad (8)$$

$$s(im, im') = \frac{\sigma_{imim'} + C_3}{\sigma_{im}\sigma_{im'} + C_3} \quad (9)$$

$$\mu_{im} = \frac{\sum_{x=1}^M \sum_{y=1}^N \sum_{z=1}^O im_{xyz}}{MNO} \quad (10)$$

$$\sigma_{im}^2 = \frac{\sum_{x=1}^M \sum_{y=1}^N \sum_{z=1}^O (im_{xyz} - \mu_{im})^2}{MNO} \quad (11)$$

$$\sigma_{im, im'} = \frac{\sum_{x=1}^M \sum_{y=1}^N \sum_{z=1}^O (im_{xyz} - \mu_{im})(im'_{xyz} - \mu_{im'})}{MNO} \quad (12)$$

$$\mu_{im'} = \frac{\sum_{x=1}^M \sum_{y=1}^N \sum_{z=1}^O im'_{xyz}}{MNO} \quad (13)$$

$$\sigma_{im'}^2 = \frac{\sum_{x=1}^M \sum_{y=1}^N \sum_{z=1}^O (im'_{xyz} - \mu_{im'})^2}{MNO} \quad (14)$$

Where M and N represent the image resolution and O denotes the number of image channels.

After conducting validation tests on both our model and Baluja's model, we compiled the results in Table 1. Table 1 provides a detailed comparison between the two approaches, highlighting the strengths and weaknesses of each. It allows for a clearer understanding of how the models perform across various metrics. We can see that our model is much better than the Baluja one. Indeed, the proposed model has slightly higher PSNR, SSIM, and UIQI values than the Baluja model, indicating better preservation of image quality. In addition, our model has significantly lower BRISQUE scores, indicating better stego image quality. Overall, the proposed model offers better image quality preservation.

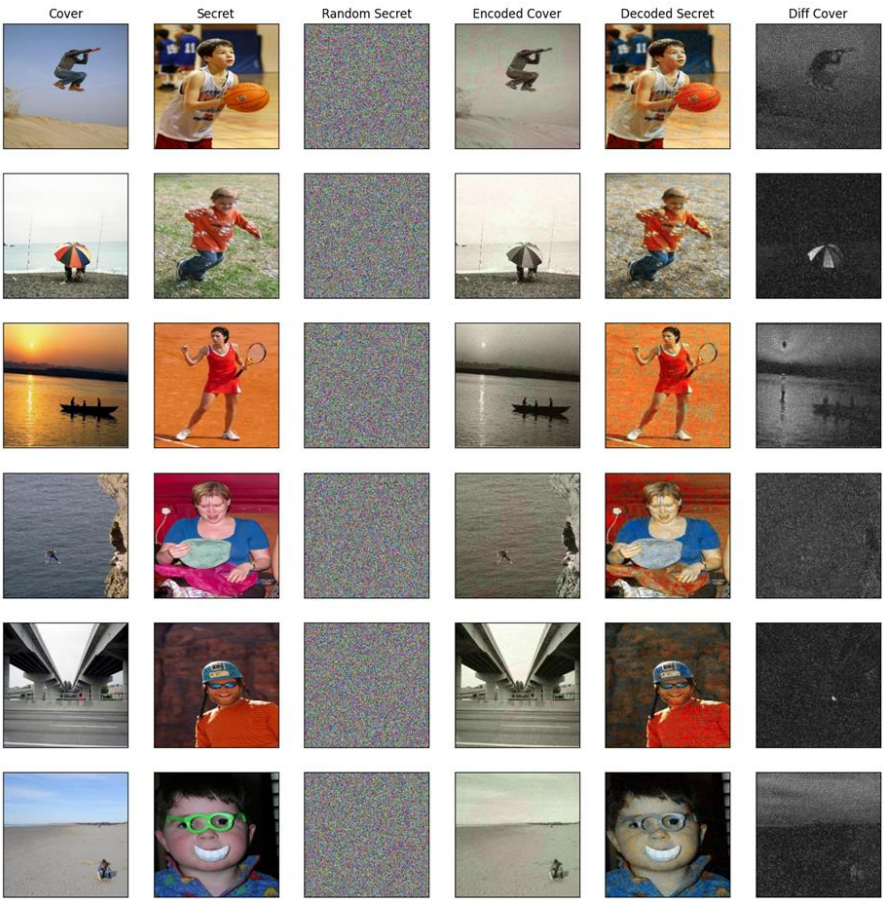


Figure 5. Results of the proposed model

Table 1. Comparative analysis of our model and Baluja's model based on validation tests

Metrics	Baluja's model	Our model
PSNR	83.6284	84.8693
SSIM	0.92224	0.94717
UIQI	78.62901	82.43392
BRISQUE_SCORE	19.73211	7.39974

In addition, our model can embed two secret images into a cover image, as demonstrated in Figure 6. It can also extract these images in real-time. Figure 6 presents two examples illustrating the success of the hiding and extraction process. In the first column, the cover image is shown, followed by secret images in columns two and three. The fourth column displays the stego image (the cover image with the hidden secret images), while columns five and six show the extracted secret images.



Figure 6. Example of hiding two secrets in one cover

4. CONCLUSION

In this paper, we present a new steganographic model for hiding multiple secret images in a cover image. To implement our model we combine a real secret image with a randomly generated pixel image. This approach enables better dissimulation of the secret image features in the difference between the original cover image and the stego image. Our contribution offers promising possibilities for hiding sensitive information while maintaining the natural appearance of the cover image. This work can be exploited in the field of intelligent advertising used in football match panels, which are used to display different advertisements according to the needs of spectators and local businesses.

ACKNOWLEDGEMENTS

The author would like to express special appreciation to the Laboratory of Engineer Sciences for providing the necessary facilities and resources.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Mohamed Htiti	✓	✓		✓	✓				✓	✓				
Aziza El Ouazizi		✓							✓	✓	✓	✓		
Ismail Akharraz		✓								✓	✓	✓	✓	
Abdelaziz Ahaitouf		✓								✓	✓	✓	✓	

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. Authors state no conflict of interest.

INFORMED CONSENT

Informed consent was obtained from all individuals included in this study.

DATA AVAILABILITY

The data that support the findings of this study are available on request from the corresponding author, [M. H.].

REFERENCES

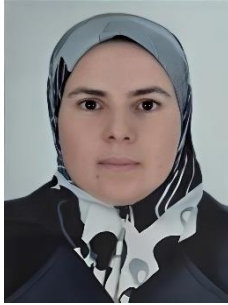
- [1] P. V. Sanivarapu, K. N. V. P. S. Rajesh, K. M. Hosny, and M. M. Fouda, "Digital watermarking system for copyright protection and authentication of images using cryptographic techniques," *Applied Sciences*, vol. 12, no. 17, Aug. 2022, doi: 10.3390/app12178724.
- [2] N. Sharma, Prabhjot, E. H. Kaur, "A review of information security using cryptography technique," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 4, pp. 323–326, 2017, doi: 10.26483/ijarcs.v8i4.3760.
- [3] A. M. Khalaf and K. Lakhtaria, "A review of steganography techniques," *AIP Conference Proceedings*, vol. 3051, no. 1, 2024, doi: 10.1063/5.0191705.
- [4] M. C. Kasapbasi, "A new chaotic image steganography technique based on huffman compression of Turkish texts and fractal encryption with post-quantum security," *IEEE Access*, vol. 7, pp. 148495–148510, 2019, doi: 10.1109/ACCESS.2019.2946807.
- [5] M. M. S. A. Al-Momin, I. A. Abed, and H. A. Leftah, "A new approach for enhancing LSB steganography using bidirectional coding scheme," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 6, Dec. 2019, doi: 10.11591/ijece.v9i6.pp5286-5294.

- [6] R. Kumar and A. Malik, "Multimedia information hiding method for AMBTC compressed images using LSB substitution technique," *Multimedia Tools and Applications*, vol. 82, no. 6, pp. 8623–8642, Mar. 2023, doi: 10.1007/s11042-022-14221-z.
- [7] A. K. Sahu and G. Swain, "Reversible image steganography using dual-layer LSB matching," *Sensing and Imaging*, vol. 21, no. 1, Dec. 2020, doi: 10.1007/s11220-019-0262-y.
- [8] S. Arivazhagan, W. S. L. Jebarani, S. T. Veena, and E. Amrutha, "Extraction of secrets from LSB stego images using various denoising methods," *International Journal of Information Technology*, vol. 15, no. 4, pp. 2107–2121, Apr. 2023, doi: 10.1007/s41870-023-01265-z.
- [9] O. P. Singh, K. N. Singh, N. Baranwal, A. K. Agrawal, A. K. Singh, and H. Zhou, "HIDemarks: hiding multiple marks for robust medical data sharing using IWT-LSB," *Multimedia Tools and Applications*, vol. 83, no. 8, pp. 24919–24937, Aug. 2023, doi: 10.1007/s11042-023-16446-y.
- [10] P. Naveen and R. Jayaraghavi, "Image steganography method for securing multiple images using LSB-GA," *Wireless Personal Communications*, vol. 135, no. 1, pp. 1–19, Mar. 2024, doi: 10.1007/s11277-024-10945-3.
- [11] P. N. Andono and D. R. I. M. Setiadi, "Quantization selection based on characteristic of cover image for PVD Steganography to optimize imperceptibility and capacity," *Multimedia Tools and Applications*, vol. 82, no. 3, pp. 3561–3580, Jan. 2023, doi: 10.1007/s11042-022-13393-y.
- [12] W.-B. Lin, T.-H. Lai, and K.-C. Chang, "Statistical feature-based steganalysis for pixel-value differencing steganography," *EURASIP Journal on Advances in Signal Processing*, vol. 2021, no. 1, Dec. 2021, doi: 10.1186/s13634-021-00797-5.
- [13] G. Paul, S. K. Saha, and D. Burman, "A PVD based high capacity steganography algorithm with embedding in non-sequential position," *Multimedia Tools and Applications*, vol. 79, no. 19–20, pp. 13449–13479, May 2020, doi: 10.1007/s11042-019-08178-9.
- [14] A. O. Modupe, A. E. Adedoyin, and A. O. Titilayo, "A comparative analysis of LSB, MSB and PVD based image steganography," *International Journal of Research and Review*, vol. 8, no. 9, pp. 373–377, Sep. 2021, doi: 10.52403/ijrr.20210948.
- [15] R. Kaur and B. Singh, "A robust and imperceptible n-ary based image steganography in DCT domain for secure communication," *Multimedia Tools and Applications*, vol. 83, no. 7, pp. 20357–20386, Aug. 2023, doi: 10.1007/s11042-023-16330-9.
- [16] M. Baziyad, T. Rabie, I. Kamel, and M. Benkhelifa, "Polynomial fitting: enhancing the stego quality of DCT-based steganography schemes," *Multimedia Tools and Applications*, vol. 81, no. 30, pp. 43999–44019, Dec. 2022, doi: 10.1007/s11042-022-13004-w.
- [17] X. Song, C. Yang, K. Han, and S. Ding, "Robust JPEG steganography based on DCT and SVD in nonsampled shearlet transform domain," *Multimedia Tools and Applications*, vol. 81, no. 25, pp. 36453–36472, Oct. 2022, doi: 10.1007/s11042-022-13525-4.
- [18] R. Patel, K. Lad, M. Patel, and M. Desai, "An efficient DCT-SBPM based video steganography in compressed domain," *International Journal of Information Technology*, vol. 13, no. 3, pp. 1073–1078, Jun. 2021, doi: 10.1007/s41870-021-00648-4.
- [19] D. Baby, J. Thomas, G. Augustine, E. George, and N. R. Michael, "A novel DWT based image securing method using steganography," *Procedia Computer Science*, vol. 46, pp. 612–618, 2015, doi: 10.1016/j.procs.2015.02.105.
- [20] A. Y. Darani, Y. K. Yengejeh, G. Navarro, H. Pakmanesh, and J. Sharafi, "Optimal location using genetic algorithms for chaotic image steganography technique based on discrete framelet transform," *Digital Signal Processing*, vol. 144, Jan. 2024, doi: 10.1016/j.dsp.2023.104228.
- [21] A. Martín, A. Hernández, M. Alazab, J. Jung, and D. Camacho, "Evolving generative adversarial networks to improve image steganography," *Expert Systems with Applications*, vol. 222, Jul. 2023, doi: 10.1016/j.eswa.2023.119841.
- [22] S. Baluja, "Hiding images in plain sight: deep steganography," *Advances in neural information processing systems*, vol. 30, 2017, pp. 2066–2076.
- [23] S. Baluja, "Hiding images within images," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 42, no. 7, pp. 1685–1697, Jul. 2020, doi: 10.1109/TPAMI.2019.2901877.
- [24] K. Sharma, A. Aggarwal, T. Singhania, D. Gupta, and A. Khanna, "Hiding data in images using cryptography and deep neural network," *Journal of Artificial Intelligence and Systems*, vol. 1, no. 1, pp. 143–162, 2019, doi: 10.33969/ais.2019.11009.
- [25] D. R. I. M. Setiadi, S. Rustad, P. N. Andono, and G. F. Shidik, "Digital image steganography survey and investigation (goal, assessment, method, development, and dataset)," *Signal Processing*, vol. 206, 2023, doi: 10.1016/j.sigpro.2022.108908.
- [26] P. Yadav and S. Dhall, "Comparative analysis of steganography technique for information security," *International Journal of Mathematical Sciences and Computing*, vol. 6, no. 4, pp. 42–69, 2020, doi: 10.5815/ijmsc.2020.04.05.
- [27] V. Himthani, V. S. Dhaka, M. Kaur, G. Rani, M. Oza, and H.-N. Lee, "Comparative performance assessment of deep learning based image steganography techniques," *Scientific Reports*, vol. 12, no. 1, Oct. 2022, doi: 10.1038/s41598-022-17362-1.
- [28] D. R. I. M. Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography," *Multimedia Tools and Applications*, vol. 80, no. 6, pp. 8423–8444, Mar. 2021, doi: 10.1007/s11042-020-10035-z.

BIOGRAPHIES OF AUTHORS



Mohamed Htiti    received the B.Sc. degree in nuclear physics from Sidi Mohamed Ben Abdallah University, in 2002. Received the M.Sc. degree in physics and nuclear techniques from Cadi Ayyad University, in 2005. Received the B.Sc. degree in IT Engineering from Faculty of Taza Polydiscipline, University of Sidi Mohamed Ben Abdallah, in 2020. Received a specialized master's degree in intelligent and mobile systems from the Faculty of Taza Polydiscipline, Morocco, in 2023. Now he is a Ph.D. student registered in the LSI Laboratory of Engineer Sciences of the Faculty of Taza Polydiscipline, University of Sidi Mohamed Ben Abdallah, Fez, Morocco. His research interests include cryptography, steganography, deep learning, and image processing. He can be contacted at email: mohamed.htiti1@usmba.ac.ma.



Aziza El ouaazizi    received her Ph.D. at University of Sidi Mohamed Ben Abdellah in 2000. After working as a Professor in Technical High School of Fes (2001), she is currently working for Professor in the Informatics at University of Sidi Mohamed Ben Abdallah, Fez. She is also a permanent member of Artificial Intelligence Data Sciences and Emergent Systems Laboratory and an associate member of Engineering Science Laboratory. Her research interests include machine and deep learning, artificial vision and image processing, pattern recognition, data analysis, evolutionary algorithms, and their applications. She can be contacted at email: aziza.elouaazizi@usmba.ac.ma.



Ismail Akharraz    received his master and Ph.D. degrees in number theory from the University of Sidi Mohamed Ben Abdellah Fez, Morocco, in 2000. From 2003 to 2020, he was at the University of Sidi Mohamed Ben Abdellah Fez, as permanent professor and permanent member of the Laboratory of Engineering Sciences. From 2021, he joined University of Ibn Zohr, Agadir Morocco, as a permanent professor and permanent member of the Laboratory of Mathematical and Informatic Engineering. His current areas of research are error-correcting codes and cryptography, intelligent systems, and recommendation systems. He can be contacted at email: ismail.akharraz@usmba.ac.ma.



Abdelaziz Ahaitouf    received his physics diploma at the University of Moulay Ismail Meknes. From 1995 to 1999, he received his M.D. and Ph.D. degrees in electronics from the University of Metz, France. In 2000, he worked in a postdoctoral position on the development of a SOI fully and partially depleted process at the Swiss Federal Institute of Technology (EPFL), Switzerland. From 2003, he joined the University of Sidi Mohamed Ben Abdellah Fez, Morocco where he is teaching in the field of electronic and IC manufacturing. He is currently working in the field of microelectronics, electrical device characterization, intelligent systems, and LDPC encoding/decoding. He can be contacted at email: abdelaziz.ahaitouf@usmba.ac.ma.